Factiva Page 1 of 3

Help

Return to Headlines

## $\mathit{The}$ Guardian

Special investigation - Race to save new victims of child porn - Computer file sharing has sent ...

By Audrey Gillan.
1,883 words
4 November 2003
The Guardian
1
English
© Copyright 2003. The Guardian. All rights reserved.

Special investigation - Race to save new victims of child porn - Computer file sharing has sent **paedophile** demand for real-time images soaring. But, as Audrey Gillan reports, police can often only watch as children grow older and continue to be abused.

Paedophiles are swapping thousands of hardcore images of child sex abuse in a new form of computer child pornography that police believe is feeding a demand for more real-time victims of abuse.

The Guardian has established that the demand for child porn through the use of file-sharing technology - normally associated with swapping music and movies - has grown so rapidly that law enforcement agencies are now employed in a global race to track down the children who are being abused. Some of the children, police believe, are being abused on a daily basis to provide a constant supply of new computerised material.

Senior officers have revealed that the scale of peer-to-peer traffic in illegal images of children now dwarfs almost any other **paedophile** network they have encountered. The images are generally more extreme and at least 20% of the users are what police class as Category One, meaning that the suspect is "of significant risk to children".

But resources available to police to tackle peer-to-peer child porn are limited and though they are catching some offenders, it may take months or even years to track down the location of some victims. In such cases, officers monitoring the images can only watch as the children grow older and continue to be abused.

Many of those addicted to child porn have flocked to peer-to-peer file sharing software such as KaZaA, Morpheus and Grokster because they are free so, crucially, users do not have to leave any credit card details, leading them to believe that they cannot be traced. The explosion in file sharing, driven by the demand for music files, has also made the technology readily accessible, quick and easy to use.

It also has the attraction of not requiring the users to be part of a traditional organised **paedophile** ring using password-protected, covert means to distribute images; rather peer-to-peer technology allows them direct access into the hard drives of other paedophiles' computers with no third party authority monitoring content as is the case with chat rooms and news groups.

Scotland Yard officers have told the Guardian that they stumbled across this phenomenon by accident during another inquiry and say they have been stunned by its exponential growth. They believe the phenomenon is more alarming than previous internet-related cases, such as the high-profile Operation Ore.

The Met's child protection hi -tech crime unit has already built a list of 800 suspects involved in file swapping illegal images in the UK alone. While most are involved only in sharing or downloading the images, a significant proportion are active abusers producing the material themselves, often using their own children, their neighbour's children or - in rarer cases - by luring strangers. At least 30 peer-to-peer cases in the UK so far involved hands-on abuse in which the children in the images were real-time victims.

Police found one man who had wired webcams into his daughter's bedroom so that he could share video images of his abuse with other peer-to-peer file sharers.

Detective Superintendent Peter Spindler, who heads Scotland Yard's **paedophile** unit, said: "We are finding real-time live abusers. These people are able to get brand new images straight up on the net." His officers have found that when new images appear, the children involved are often related to or live nearby the person distributing the material.

But the sheer volume of new material, combined with the fact that it could have been produced anywhere in the world, has meant that police have often been unable to pinpoint the child's location.

Factiva Page 2 of 3

Detectives rely on two methods of tracing location: electronic footprints left by the user while online and forensic analysis of the images to find clues pointing to the country of origin, such as telephone books in the background or the style of furnishings. In some cases, often where the child is being held prisoner and abused in a completely blank room, there are not enough leads for police to chase.

One case being investigated involves a prepubescent girl who is being held prisoner in a room and repeatedly abused. International law enforcement agencies know only that she is in the United States and the FBI is trying to pinpoint her exact location. New images of the child are shared through KaZaA and other services but police have been unable to find her.

Gemma Holland, victim identification project manager at the University of Cork's Combating **Paedophile** Information Networks in Europe (Copine), which has a database of more than 600,000 child porn images, said: "This is a global problem. The abuse could be in the next village or somewhere near you but the problem is the images are being shown globally. Identifying the kids in these images should be our prime concern and of the greatest importance."

The decentralised nature of the internet and peer-to-peer specifically make it difficult to define numbers of images in circulation, or children involved, but experts say it is growing daily. Washington's national centre for missing and exploited children, which acts as a clearing house for child porn tip-offs, said that reports of such images in shared files had increased by 400% this year.

David Wilson, professor of criminology at the University of Central England in Birmingham, said: "Peer-to-peer facilitates the most extreme, aggressive and reprehensible types of behaviour that the internet will allow."

The Guardian understands that the National Crime Squad is considering coordinating all of this work, rather than leaving it to small groups working within the country's various forces; so far the leading forces have been the Met, West Midlands and Greater Manchester.

Peer-to-peer has become more attractive for paedophiles in the wake of Operation Ore, the high-profile British police operation which was launched after US authorities handed over the names of 7,200 people suspected of subscribing to websites offering paedophilic images. While Ore has grabbed headlines, many senior officers and child abuse experts believe that targeting people at the lower end of the **paedophile** spectrum has been a distraction in terms of child protection.

Prof Wilson believes Ore showed how the criminal justice system concentrated on the wrong type of offender, the people who downloaded the material rather than produced them. It needed to refocus on activities such as peer-to-peer file sharing and the producers of child pornography.

He said: "Police operations have not been getting to the type of **paedophile** that we need to get to. It's in their interests to keep the debate moving towards the kind of people they should be spending time and resources on.

"The achilles heel of peer-to-peer is that it makes something that is secret and furtive into something that is public and when it is public that offers the police a window of opportunity to police it."

In a room on the fifth floor at Scotland Yard, officers in the hi-tech crime unit are trying to do exactly that, sitting at com puters, monitoring activity on the peer-to-peer boards. They are part of a team working on Operation Pilsey, which started as a small-time inquiry in March 2001 by the Met's clubs and vice unit and burgeoned with the number of people posting images via file sharing. The detectives working here are now inundated.

They explain that they can use technology to detect the location of those who download the images and sometimes that of the abusers. If there is a child immediately in danger, officers will conduct a raid as soon as they have a location.

Paedophiles believe it is harder for them to be detected through peer-to-peer software but investigators are able to access their shared folders and quickly discover if they contain illegal images of child abuse. They are then able to establish the location of the owner of the shared folder.

## Extreme

Detective Constable Sean Robbie scans through a list of images held in one shared folder to illustrate the point. A scroll through shows the thousands of illicit files that are on offer. Some of the milder titles are "Nine-year-old rape", "Eight-year dance" and "Dad does daughter". All of it is accessible to anyone who requests it, including children. Key in the word Britney or Barbie and the number of images available is astonishing.

We view one of the files involving the American girl - of which there are thousands - and see her dancing provocatively for the camera. This is one of the least extreme of the images available, some of them replications, others new.

Over the last 18 months, Pilsey officers have found a surprising number of magistrates, city workers and police officers, and even children, with **paedophile** images on their computer. Two weeks ago, William Legros, now 18 but 16 when he downloaded child sex images, was given a 12-month community rehabilitation or der after being tracked down by Pilsey.

Factiva Page 3 of 3

James Taylor, 43, was convicted in Scotland last month after he posted digital camera shots of himself raping a 13-month-old baby. He was detected when Scotland Yard officers passed his details on to local police. Forensic analysis of the images helped establish the baby's location in a house nearby.

Taylor, from Grangemouth, who is married with children aged 15, 13 and 11, also took indecent pictures of a six-year-old child as she slept and had 2,880 hardcore child porn images on his hard drive. He was sentenced to just five years.

In June, Gordon Sheppard, 35, of Stirling, was convicted of posting more than 900 pictures of himself abusing an eight-year-old. He is now serving seven years.

"No matter how many we nick, there doesn't seem to be any marked disruption of them," one detective told the Guardian.

Detective Inspector Brian Ward, the officer in charge of Pilsey, said: "So many computers are being examined and so many suspects are being thrown up. We are in danger of being inundated. We have a department of 22 and it's not enough. We have got to start thinking more about the disruption of this."

By exposing themselves to public gaze via file swapping services, paedophiles whose abuse may never have come to light are now more likely to be caught. But with communications technology developing so rapidly, detectives know that their success in bringing down peer-to-peer child porn networks will quickly drive the users to find new and more sophisticated distribution means.

John Carr, internet adviser to the children's charity NCH Action for Children, has warned that encoding of their material may be the paedophiles' next bolthole.

For Det Insp Ward, the challenge will be to ensure that by the time the child pornographers get that far, his officers are already there waiting for them.

Document GRDN000020031104dzb40008v

Return to Headlines

factiva © 2003 Factiva, Dow Jones & Reuters